IMPLEMENTASI ENKRIPSI DATA BERBASIS VIRTUAL PRIVATE NETWORK DI KANTOR PADANG EKSPRES

TUGAS AKHIR

Diajukan sebagai salah satu syarat
untuk memperoleh gelar Ahli Madya

Oleh

RISSA YULANDA

BP: 06 092 051

Program Studi Teknik Komputer
Jurusan Teknologi Informasi
Politeknik Universitas Andalas

2009

ABSTRAK

Teknologi *Virtual Private Network* cocok digunakan untuk perusahaan-perusahaan yang mempunyai beberapa cabang dan menginginkan transaksi data yang aman. *Virtual Private Network* [VPN] merupakan cara untuk membuat suatu jaringan bersigat *private* dan aman dengan menggunakan jaringan *public*. Adanya VPN dapat mengirim data antara dua komputer yang melewati jaringan public sehingga seolah-olah terhubung secara *point to point*. Disaat kantor Pusat melakukan transaksi data dengan kantor cabangnya yang didalam nya terdapat rahasia perusahaan, dikhawatirkan adanya pihak yang tidak bertanggung jawab merusak atau menyabotase data tersebut. Baik *hacker* maupun virus yang ditanamkan dalam jaringan tersebut.

Dengan menambahkan suatu program yang menggunakan metode ROT 13 akan dihasilkan keamanan data yang lebih *secure* karena selain adanya enkripsi dari VPN sendiri untuk mengamanan dalam jaringan, file data pun sudah teracak lagi dengan menggunakan Metode ROT 13. Adapun perancangannya dimulai dari topologi jaringan VPN, pemilihan sistem operasi, instalasi dan konfigurasi mikrotik VPN di Kantor Padang Ekspres. Selain itu juga ditulis mengenai langkah-langkah implementasi enkripsi data.

Jadi kedua teknologi ini dapat dipadukan untuk mendapatkan hasil yang sempurna, yaitu komunikasi data aman dan efisien. Aman berarti data tetap terjaga kerahasiaan dan keutuhannya. Tidak sembarang pihak dapat menangkap dan membaca data, meskipun data tersebut lalu-lalang di jalur komunikasi publik.

Kata kunci: Teknologi *Virtual Private Network*, Program untuk Keamanan Data.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Namun masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan yang terakhir dalam daftar yang dianggap penting. Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi yang diinginkan hanya boleh diakses oleh orang – orang tertentu. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi.

Terhubungnya LAN atau komputer ke internet membuka potensi adanya lubang keamanan *(security hole)* yang tadinya ditutupi dengan mekanisme keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan dan kenyamanan dalam mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Semakin tinggi tingkat keamanan, semakin sulit atau tidak nyaman untuk mengakses informasi.

Dari hal tersebut, teknologi *virtual private network* (VPN) merupakan suatu bentuk jaringan privat yang melalui jaringan publik (internet) dengan menekankan pada keamanan data dan akses global melalui internet. Hubungan ini dibangun melalui suatu tunnel (terowongan) *virtual* antara 2 *node*. Dengan menggunakan jaringan publik ini, *user* dapat tergabung dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti ketika *user* berada dalam kantor. Data dienkapsulasi (dibungkus) dengan *header* sehingga data sampai ke tujuan. Dengan adanya koneksi

bersifat *private*, data yang dikirimkan terlebih dahulu dienkripsi untuk menjaga kerahasiaanya. Sehingga paket tertangkap ketika melewati jaringan publik tidak terbaca karena proses enkripsi. Sebuah Instansi seperti Padang Ekspres membutuhkan sebuah keamanan jaringan untuk menjaga privasi dan otentikasi dalam transaksi datanya.

Yang mana ada saat sekarang ini, berbagai cara orang ingin memasuki sebuah jaringan orang lain, untuk melakukan apa saja sesukanya. Jika hal ini terjadi, tentu saja dapat menjatuhkan citra sebuah Instansi seperti Padang Ekspres. Apalagi jika berhubungan dengan asset berharga dari perusahaan. Untuk itu perlu dilakukannya enkripsi data dalam keamanan jaringan, agar karyawan ataupun pihak perusahaan Padang Ekspres dapat bekerja dengan aman dan cepat serta menjamin kerahasiaan dari perusahaan pada saat transaksi data.

Berdasarkan permasalahan tersebut, maka dilakukan pengkajian dan pembahasan yang dituangkan dalam bentuk tugas akhir dengan judul :

"IMPLEMENTASI ENKRIPSI DATA BERBASIS VIRTUAL PRIVATE NETWORK (VPN) DI KANTOR PADANG EKSPRES".

1.2 Rumusan Masalah

Permasalahan yang dihadapi dalam pembuatan tugas akhir ini adalah mengimplementasi enkripsi data di Kantor Padang Ekspres dan menguji keefektifan VPN sebagai tingkat *security* yang lebih baik. Maka didapat rumusan permasalah sebagai berikut:

a. Bagaimana sistem kerja dari sistem keamanan jaringan VPN di Kantor Padang Ekspres?

b. Bagaimana merancang dan menerapkan program aplikasi enkripsi data menggunnakan metode ROT 13?

c. Bagaimana cara instalasi dan konfigurasi system operasi mikrotik?

d. Bagaimana mengkofigurasi jaringan VPN di Padang Ekspres?

e. Bagaimana bentuk pengamanan data sebelum dan sesudah program aplikasi enkripsi dan deskripsi di terapkan?

1.3 Tujuan

Tujuan yang ingin dicapai dalam penulisan Tugas Akhir ini adalah sebagai berikut:

a. Merancang suatu sistem yang dapat digunakan untuk *security* pada jaringan VPN.

b. Mengimplementasikan enkripsi data dalam transaksi data di Kantor Padang Ekspres.

c. Untuk lebih memahami dan mengimplementasikan enkripsi data.

d. Untuk lebih memahami cara instalasi dan konfigurasi mikrotik pada VPN.

e. Mengamankan data sampai ke tujuan selama berada dalam jalur internet.

1.4 Batasan Masalah

Adapun batasan masalah yang akan dikaji dalam penulisan tugas akhir ini adalah sebagai berikut:

a. Mengetahui sistem kerja dan topologi VPN di Padang Ekspres.

b. Mengetahui aplikasi program Visual Basic yang menggunakan metoda ROT 13.

BAB V

PENUTUP

5.1 Kesimpulan

a. Melalui mikrotik dapat dilihat *source address*, *destination address* serta *Port* dari suatu paket data yang telah dilalui dalam jaringan VPN. Tidak hanya itu melainkan kita dapat melihat aktivitas suatu paket sedang dalam kondisi apa dan apa yang sedang diperlakukan pada suatu paket, apakah di *forward, drop* dan lain-lain.

b. Dalam sistem keamanan pada jaringan VPN enkripsi data dilakukan Selama masa komunikasi data, perangkat jaringan memiliki kemampuan enkripsi jenis ini akan mengubah data yang berupa teks murni (cleartext) menjadi berbentuk teks yang telah diacak atau istilahnya adalah ciphertext. Teks acak ini tentu dibuat dengan menggunakan algoritma. Teks acak ini sangat tidak mudah untuk dibaca, sehingga keamanan data tetap terjaga.

c. Implementasi enkripsi data dengan menggunakan metode ROT 13 dalam transaksi data dalam jaringan VPN. Kedua teknologi ini dapat dipadukan untuk mendapatkan hasil yang sempurna, yaitu komunikasi data aman dan efisien. Aman berarti data tetap terjaga kerahasiaan dan keutuhannya. Tidak sembarang pihak dapat menangkap dan membaca data, meskipun data tersebut lalu-lalang di jalur komunikasi publik. Keutuhan yang tetap terjaga maksudnya tidak sembarang orang dapat mengacaukan isi dan alur data. Hal ini perlu dijaga karena jika sudah lewat jalur publik, banyak sekali orang iseng yang mungkin saja menghancurkan data di tengah jalan.

DAFTAR PUSTAKA

Iwan Sofana. 2008. *Membangun Jaringan Komputer*.Bandung.Informatika

http://ilmukomputer.org/category/jaringan-komputer

http://putrianitautami.blogspot.com/2009/06/pengertian-mikrotik-router-os.html

www.putty.nl

http://www.ittelkom.ac.id/library/index.php?view=article&catid=10%3Ajaringan&id=436%3A-mikrotik-&option=com_content&Itemid=15

http://artikelkuliah.blogspot.com/2009/06/virtual-private-network.html

http://dedenthea.wordpress.com/2007/02/01/apa-itu-vpn/

http://sandi.math.web.id/?p=101